APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/801,614	03/08/2001	Gerald Francis McBrearty	AUS9-2000-0935-US1	5324

7590 12/15/2005	**EXAMINER**
International Business Machines Corporation	LEZAK, ARRIENNE M
Intellectual Property Law Department	

ART UNIT	PAPER NUMBER
2143	

International Business Machines Corporation
Intellectual Property Law Department
Internal Zip 4054
11400 Burnet Road
Austin, TX 78758

DATE MAILED: 12/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

DEC 1 5 2005

Technology Center 2100

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/801,614
Filing Date: March 08, 2001
Appellant(s): MCBREARTY ET AL.

_____

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11 October 2005 appealing from the Office action mailed 5 May 2005.

1.   **Real Party in Interest**

A statement identifying the real party in interest is contained within the brief.

2.   **Related Appeals and Interferences**

A statement indicating Applicant is unaware of any related appeals or

interferences is contained within the brief.

3.   **Status of Claims**

The statement of the status of the claims contained within the brief is correct.

4.   **Statement of Amendments After Final**

The Appellant's statement of the status of amendments after final rejection

contained within the brief is correct.

5.   **Summary of Invention**

The summary of the invention contained within the brief is correct.

6.   **Issues – Grounds of Rejection to Be Reviewed on Appeal**

The Appellant's statement of the issues within the brief is correct.

7.   **Claims Appealed**

The copy of the appealed claims contained in the Appendix to the brief is correct.

8.   *Prior Art of Record*

Examiner relied upon the following prior art in the rejection of the claims under

appeal:

US Patent 5,933,498	Schneck	11-1997
US Patent 6,351,811 B1	Groshon	04-1999

9.   *Grounds of Rejection*

1.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2.   Claims 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27 & 30 rejected under 35 U.S.C.

103(a) as being unpatentable over US Patent 5,933,498 to Schneck in view of US

Patent US 6,351,811 B1 to Groshon.

3.   Regarding Newly Amended Claims 1, 3, 5, 7, 10, 14, 17, 21, 25 & 27, Schneck

discloses a data processing operation, (Col. 10, lines 14-26), communication network or

world wide web communication network, (Col. 14, lines 66-67 & Col. 15, lines 1-13),

having stored data in a plurality of data files, (Col. 7, lines 27-36), a system, method and

computer program having code recorded on a computer readable medium for protecting

said data files from unauthorized users, (Abstract & Col. 7, lines 40-45), comprising:

-          means for receiving user requests for access to data files, (Col. 15, lines

19-67; Col. 16, lines 1-59; and Col. 17, lines 54-59);

- means for determining whether said requests are unauthorized intrusions into said requested data files, (Col. 15, lines 19-67; Col. 16, lines 1-59; and Col. 17, lines 54-59); and

- means responsive to a determination that a request is unauthorized for destroying the requested data files, (Col. 7, lines 44-45; Col. 8, lines 26-28; Col. 15, lines 20-67; Col. 16; and Col. 17, lines 1-59).

4.   Though Schneck teaches a storage capability for data, (Schneck - Col. 7, lines 27-36), Schneck does not specifically teach storing for each of said plurality of data files, a backup file inaccessible to user requests. Groshon discloses a system and method for controlling the transmission of data in a computer network, (Groshon - Abstract), wherein backup copies are stored, which backup copies can be encrypted to provide additional security, (Groshon – Col. 4, lines 64-67 & Col. 5, lines 1-9).

5.   It would have been obvious to one of ordinary skill in the art at the time of invention by Applicant to include backup copies of the data within the Schneck system. The motivation to combine would be an obvious preventative measure within a communication network with a storage capability wherein it is understood that data may be compromised, (Groshon – Col. 2, lines 29-34), and thus it would be obvious to have un-compromised copies available as needed. Moreover, Groshen teaches additional security measures for the backup data wherein it would be obvious that said additional security would serve to limit access to the backup data, and wherein it would be obvious that the backup copies would not be available to a random user, especially within a system capable of tamper detection.

6.   Though Schneck teaches a storage capability for data, (Schneck - Col. 7, lines

27-36), Schneck does not specifically teach a means for reloading a backup file for each

destroyed file. As noted above, Groshon discloses a system and method for controlling

the transmission of data in a computer network, (Groshon - Abstract), wherein backup

copies are stored, which backup copies can be encrypted to provide additional security,

(Groshon – Col. 4, lines 64-67 & Col. 5, lines 1-9). Examiner notes that within a tamper

detection system that destroys data upon tamper detection, (like Schneck), It would

have been obvious to reload said backup copies for purposes of recreating the

destroyed file, as the ability to recreate the original data is a necessity for all other users

of the system reliant upon the same. Thus, Newly Amended Claims 1, 3, 5, 7, 10, 14,

17, 21, 25 & 27 are found to be unpatentable over the combined teachings of Schneck

in view of Groshon.

7.   Regarding Original Claims 4, 13, 20, 24 & 30, Schneck in view of Groshon is

relied upon for those teachings disclosed herein. Schneck further discloses a means for

determining whether said user requests are unauthorized intrusions, which means

include: means for determining whether a user access identification code has been

denied; and means for determining whether the user has copied the requested files,

(Col. 15, lines 19-57; Col. 16; and Col. 17, lines 1-59). Examiner notes that the access

mechanism in Schneck specifically provides a means for preventing unauthorized

access and for tamper protection and detection. A means for preventing unauthorized

access would obviously include a determination of authority via a user access

identification code, (as obviously necessitated by access rules, (Abstract)). Further, a

means for determining whether user has copied requested files, (accessing data – Col.

17, lines 54-59), would obviously be included within a tamper detection/reset

mechanism as one of many forms of determining a rule violation. Thus, Original Claims

4, 13, 20, 24 & 30 are found to be unpatentable over the combined teachings of

Schneck in view of Groshon.

10.   *Response to Arguments*

   10.1   Rejection of Claims 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27 & 30

      10.1.A   The combined teachings of the Schneck '498 reference and
      the Groshon '811 reference in fact disclose all the elements of Appellant's
      claimed invention, rendering the same obvious and unpatentable under 35
      U.S.C. 103(a), (Appeal Brief: pp. 4 & 7).

In response to Appellant's arguments against the references individually, one

cannot show nonobviousness by attacking references individually where the rejections

are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208

USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir.

1986). Specifically, Appellant has argued the references individually throughout the

Appeal Brief, and Examiner respectfully emphasizes that is the combined teachings of

the references which teach Appellant's claim limitations, in their entirety, rendering the

same unpatentable, as noted herein above and within paragraph 9 of the Final Office

Action dated 5 February 2005, which reads as follows:

> Examiner notes that Applicant has admitted that Schneck teaches destruction of data found to be
> corrupted by unauthorized intrusion, and Groshon teaches a backup network data storage, and
> that one skilled in the art could be argued to consider, from these two references, that destroyed
> data could be replaced from backup storage, (Amendment – p.12). Examiner further notes that

Groshon additionally teaches <u>storing of a control copy of the data in a database inaccessible</u> <u>through the public computer network</u>, (Col. 3, lines 24-37), and a "validation function" computed at the time of page request, (Col. 4, lines47-67 & Col. 5, lines 1-43), which validation function reads upon "an <u>initial</u> determination that a request is unauthorized" per the amended claim language. Thus, as noted herein, Examiner respectfully disagrees with Applicant's assertion that the combined teachings of Schneck in view of Groshon do not obviously disclose the implementation taught by Applicant.

Additionally, in response to Appellant's argument that Gorshon uses the control copy to determine if data has been compromised, (as opposed to Appellant's use of the control copy to determine whether a received request for data files is an unauthorized intrusion), Examiner notes that a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. In this case, Examiner maintains that the inaccessible control copy noted within the prior art clearly reads upon "a backup file inaccessible to user requests", as noted within Appellant's claim language.

More importantly, <u>Examiner notes that Appellant's claim language is completely</u> <u>silent as to the use of the backup file (control copy) for purposes of determining whether</u> <u>a received request for data files is an unauthorized intrusion</u>. Thus, in response to Appellant's argument that the references fail to show certain features of Appellant's invention, it is noted that the features upon which applicant relies (i.e., <u>the use of the</u> <u>backup file for determining</u> whether a received request for data files is an unauthorized intrusion) is not recited in the rejected claim(s). Although the claims are interpreted in

light of the specification, limitations from the specification are not read into the claims.

See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Specifically,

Examiner reiterates that the use of the inaccessible control copy clearly reads upon

Appellant's use of a backup file inaccessible to user requests, as enumerated within the

claim language. Moreover, Examiner notes that the control copies are copies of each

and every piece of data within the system; regardless of how said control copies are

stored, (i.e.: as one file or as multiple files). As noted herein, Gorshon's inaccessible

control copies clearly read upon each and every one of Appellant's backup files, (as

pertaining to one file or a plurality of files), rendering the same unpatentable.

10.1.B   Groshon '811 in fact discloses reloading of the backup file, (Appeal Brief: p.5).

Regarding Appellant's argument that the Examiner has failed to note that the

Schneck '498 reference does not disclose the reloading of the backup file feature,

(Appeal Brief – p.5), Examiner respectfully disagrees noting the Advisory Action of 10

August 2005, which enumerates the following:

> In response to Applicant's argument that Examiner fails to note that the prior art does not teach "reloading a backup file for each destroyed file", Examiner respectfully disagrees, noting paragraph 6 on p.4 of the Final Office Action dated 5 May 2005, which reads as follows:
>
> Though Schneck teaches a storage capability for data, (Schneck - Col. 7, lines 27-36), <u>Schneck does not specifically teach a means for reloading a backup file for each destroyed file</u>. As noted above, Groshon discloses a system and method for controlling the transmission of data in a computer network, (Groshon - Abstract), wherein backup copies are stored, which backup copies

can be encrypted to provide additional security, (Groshon – Col. 4, lines 64-67 & Col. 5, lines 1-9). Examiner notes that within a tamper detection system that destroys data upon tamper detection, (like Schneck), It would have been obvious to reload said backup copies for purposes of recreating the destroyed file, as the ability to recreate the original data is a necessity for all other users of the system reliant upon the same.

10.1.C   Groshon '811 does not in fact teach away from Appellant's claimed invention or Examiner's combination of elements, (Appeal Brief: p.6).

Regarding Appellant's argument that the Groshon '811 references teaches away from the Examiner's combination of elements, (Appeal Brief – p. 6), Examiner respectfully disagrees, noting that Appellant's cited portion within the Groshon '811 reference is taken out of context and in fact does not teach away from the claimed invention. Specifically, the Groshon '811 reference in fact discloses that "if a backup copy of the requested data is available, the backup copy can be transmitted", (Groshon – Col. 6, lines 31-33), which clearly indicates that the backup copy has been substituted for the original, unavailable, (i.e.: destroyed) file.

Moreover, Appellant's cited portion, (Groshon – Col. 6, lines 34-38) is specific to the needs of a specific application, and notes that should the specific application require transmission of data, (regardless if the data has been compromised), then that compromised data may be transmitted, (i.e.: under circumstances wherein a security measure includes transmission of data for purposes of reverse-tracing to find the origin of the unauthorized request). Thus, the use of the wording may be is a clear indication that such data will not always be sent, nor must be sent. That noted, Examiner

reemphasizes that the Groshon '811 reference in fact does not teach away from

Appellant's claimed invention and Examiner's combined references in fact render

Appellant's claimed invention unpatentable.

10.1.D   The combined teachings of Groshon '811 and Schneck '498 are not in fact made in light of Appellant's teachings. (Appeal Brief: p.6).

Regarding Appellant's argument that the combination of the Groshon '811 and

Schneck '498 art has been made in light of Appellant's teachings, (Appeal Brief – p.6),

Examiner respectfully disagrees noting the Advisory Action of 10 August 2005, which

enumerates the following:

> In response to applicant's argument that the examiner's conclusion of obviousness is based upon
> improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a
> sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into
> account only knowledge which was within the level of ordinary skill at the time the claimed
> invention was made, and does not include knowledge gleaned only from the applicant's
> disclosure, such a reconstruction is proper. See In re McLaughlin, 443 F.2d 1392, 170 USPQ
> 209 (CCPA 1971).

> In response to applicant's argument that there is no suggestion to combine the references, the
> examiner recognizes that obviousness can only be established by combining or modifying the
> teachings of the prior art to produce the claimed invention where there is some teaching,
> suggestion, or motivation to do so found either in the references themselves or in the knowledge
> generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d
> 1596 (Fed. Cir. 1988)and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).
> Examiner notes that proper motivation to reload backup copies is provided for in the final office
> action, and Examiner additionally notes that Groshon specifically teaches the backup of data for
> purposes of preventing transmission of compromised data in a computer network, (Col. 2, lines
> 29-46), wherein it would have been obvious and necessary to reload the backup non-

compromised files in the event compromised files had been destroyed and wherein an additional subsequent request had been made for a non-compromised copy of the files.

Examiner again emphasizes that it is the properly combined teachings of the Groshon '811 and Schneck '498 art which disclose Appellant's claim limitations in their entirety, rendering the same unpatentable, as noted herein above.

10.1.E   The combined teachings of Groshon '811 and Schneck '498 in fact render the dependant claims unpatentable, (Appeal Brief: p.8).

Regarding Appellant's argument that the dependant claims are patentable in light of the arguments made for the patentability of the independent claims, Examiner respectfully disagrees noting that Appellant's arguments regarding the independent claims have not been found to be persuasive, and as such do not render any of the claims patentable.

Additionally, Examiner notes that while Appellant admits that the "Schneck '498 reference may disclose the individual elements of rejecting or denying access ID codes or determining whether files have been copied", (Appeal Brief – p.8), Appellant argues that the reference does not teach the combination of events triggering a destruction of database files, (Appeal Brief – p.8), and Examiner respectfully disagrees noting that the Schneck '498 reference specifically enumerates, "in preferred embodiments, data are destroyed when tampering is detected", (Schneck – Col. 7, lines 44-45 & Claims 1-88 – specifically Claims 16, 17, 28, 38-41, 47, 60 & 63), and the acts of rejecting or denying access ID codes or determining whether files have been copied are clearly and

obviously means by which tampering is detected, especially within a system for

controlling access and distribution of digital property, like that of Schneck, which clearly

teaches user access to data only in accordance with the rules as enforced by a

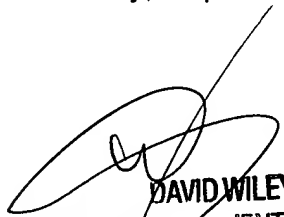mechanism protected by tamper detection, (Schneck – Abstract).

Therefore, for the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Arrienne M. Lezak

Conferees

David A. Wiley, Rupal Dharia

DAVID WILEY
SUPERVISOR PATENT EXAMINER
TECHNOLOGY CENTER 2100

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER